FAX or Internet

UNITED STATES DISTRICT COURT

for the

District of Arizona

In the Matter of the Search of: A rose colored iPhone with a purple/pink Otterbox protective case found at milepost 1 on Monument Valley Road in Monument Valley, Arizona 86033.	)	Case No. 22-4208 MB CDB

ELECTRONICALLY ISSUED SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer.

An application by a federal law enforcement officer for the government requests the search of the following person or property located in the District of Arizona
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-2

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-2

I find that the affidavit(s), or any recorded testimony, have been communicated by reliable electronic means and establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before July 7, 2022
(not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the search warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave a search warrant copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Camille D. Bibles.
(Name)

☐ I find that immediate notification may have an adverse result as specified in 18 U.S.C. §3103a (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and Time Issued: Camille D. Bibles Digitally signed by Camille D. Bibles Date: 2022.06.19 21:20:30 -07'00'
Judge's Signature

City and State: Flagstaff, Arizona Honorable Camille D. Bibles, U.S. Magistrate Judge
Printed Name and Title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing Officer's Signature

_____
Printed Name and Title

FAX or Internet

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of:

A rose colored iPhone with a purple/pink Otterbox protective case found at milepost 1 on Monument Valley Road in Monument Valley, Arizona 86033

Case No. 22-4208 MB CDB

(Original To Be Filed With Court)

ELECTRONIC APPLICATION FOR SEARCH AND SEIZURE WARRANT

I, F.B.I. Special Agent Jenifer J. Mulhollen, a federal law enforcement officer for the government, request an electronic search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-2.

located in the District of Arizona, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-2.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- [X] evidence of a crime;
- [ ] contraband, fruits of crime, or other items illegally possessed;
- [ ] property designed for use, intended for use, or used in committing a crime;
- [ ] a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1111 and 1153	Murder (Indian Country)

The application is based upon the following facts:

- [X] Continued on the attached sheet (see attached **Affidavit**).
- [ ] Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Emma Mark
Pursuant to 28 U.S.C. § 1746(2), I declare under penalty of perjury that the foregoing is true and correct.

Applicant's Signature

Jenifer J. Mulhollen, F.B.I. Special Agent
Printed Name and Title

Sworn by Telephone

Date/Time: _____

Camille D. Bibles

Digitally signed by Camille D. Bibles
Date: 2022.06.19 21:21:26 -07'00'

Judge's Signature

City and State: Flagstaff, Arizona

Camille D. Bibles,
United States Magistrate Judge
Printed Name and Title

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

ELECTRONICALLY SUBMITTED AFFIDAVIT

I, FBI Special Agent Jenifer J. Mulhollen, state under oath as follows:

1. I have been employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) since February 2013. As a SA of the FBI, I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510(7), that is, I am an officer of the United States who is authorized by law to conduct investigations of, and make arrests for, offenses enumerated in Title 18. In the course of my official duties, I am charged with the investigation of crimes occurring on the Navajo Nation Indian Reservation (Navajo Nation) within the District of Arizona. Based on my training, education, and experience, I know that the Navajo Nation is a federally recognized tribe.

2. The information contained in this affidavit comes from my personal observations, my training and experience, and information obtained from other agents, officers and witnesses.

3. Because this affidavit is being submitted for the limited purpose of establishing probable cause, your Affiant has not included every fact known to your Affiant concerning this investigation.

INTRODUCTION

4. As more fully described below, this matter involves the death investigation of J.Y., a non-native female living on the Navajo Nation Indian Reservation.

5. This affidavit supports the application for a search warrant authorizing the search of J.Y.'s residence, where she was reported deceased on June 19, 2022 as well as her cell phone. J.Y.'s body is still inside the residence, and it is believed more evidence of a crime may be found therein. There is probable cause to believe that evidence of Murder, in violation of Title 18, United States Code (U.S.C.) §§ 1111 and 1153 will be found at the residence. The residence and cell

phone are particularly described in **Attachments A-1** and **A-2**, and the evidence being sought is particularly described in **Attachments B-1** and **B-2.**

INVESTIGATION/PROBABLE CAUSE

6. On June 19, 2022, around 9:00 a.m. (Reservation Time) the Navajo Nation Kayenta Police District received a phone call from Atsashash Yellowhorse who stated he had found his mother, a non-native, deceased inside their residence. Atsashash identified his mother as J.Y. Due to J.Y.'s status as non-native, the information was given to Navajo County Deputy/FBI Task Force Officer (TFO) Nathaniel Simonson for investigation.

7. On June 19, 2022, your Affiant spoke with TFO Simonson who advised he arrived on scene, a shed located at milepost 1 on Monument Valley Road in Monument Valley, Arizona (GPS Coordinates at approximately 36.997634 -110.156118) at approximately 1:00 p.m (Reservation Time).

8. TFO Simonson interviewed Atsashash Yellowhorse on scene. Atsashash stated he and his mother, J.Y., both lived at the residence. On June 18, 2022, between 10:00 and 10:30 p.m. (Reservation Time) Atsashash left the residence for the night and his mother was home alone. Atsashash spent the night at his girlfriend, Marcia Todechedne's, house approximately 8 miles down the road. Atsashash returned home on June 19, 2022, between 8:30 and 9:00 a.m. and found the door to the residence ajar and the dogs outside. Atsashash found J.Y. unresponsive and face-down in a pillow on a couch. J.Y. was cold to the touch and her hands were above her head. J.Y.'s cell phone (TARGET PHONE) was on the floor near the couch where her body was found. Atsashash stated J.Y.'s stomach and face were blue, and her eyes were open.

9. Atsashash informed TFO Simonson they have a business called "Rent a Tent" that is advertised on Air BNB. Atsashash explained J.Y.'s cell phone was for the business, and they had surveillance footage on the property. J.Y.'s phone used an app to view the surveillance footage.

Atsashash told TFO Simonson he viewed the surveillance footage utilizing J.Y.'s phone prior to law enforcement arriving. Atsashash saw that J.Y. was outside with a flashlight between 10:00-11:00 p.m. on June 18, 2022.

10. Atsashash informed TFO Simonson there was a dispute with a neighboring business, Bigman Native Arts. He stated individuals involved in that business had threatened to kill J.Y. and/or burn her house down. Atsashash also stated there was a money in a drawer by a computer inside the residence, but there should have been more and Atsashash does not know what J.Y. did with the rest of the money. The money is revenue from their Air BNB business.

11. Atsashash told TFO Simonson he had to clean up the tents to get ready for the next Air BNB customers and departed the scene without providing consent to search the residence.

12. TFO Simonson seized J.Y.'s cell phone to preserve it as evidence. TFO Simonson conducted a safety sweep of the residence and confirmed a female was deceased on the couch. TFO Simonson did not see any visible wounds to the body and did not observe any signs of forced entry into the residence. TFO Simonson did not locate any form of identification for the deceased female.

THINGS TO BE SEARCHED FOR AND SEIZED

13. Based on the foregoing, your Affiant seeks permission to search the residence as described in **Attachment A-1** for evidence pertaining to the death investigation of J.Y. Based on your Affiant's training and experience, suspects often leave behind evidence from the commission of offenses at the location the offense was committed. Thus, your Affiant is seeking a warrant to search for evidence related to Murder, in violation of 18 U.S.C. §§ 1111 and 1153, including the deceased female body, any blood evidence, computers, and any business records related to the death investigation, as further described in **Attachment B-1**.

14. Your affiant also knows that indicia of ownership, occupancy, and/or use of a

residence is important in a criminal case. Such information may help establish the location of a crime, potential and/or likely suspects, and potential and/or likely witnesses. Based on your affiant's training and experience, indicia of ownership and occupancy includes such things as: mail (e.g., bills) that may be addressed to the occupant(s); driver's licenses and/or identification cards; personal property such as clothing that may identify the owners and/or occupants of the structure; and photographs of the owners and/or occupants at the structure.

15. Based upon the facts contained in this affidavit, your Affiant submits there is probable cause to believe that the items listed in **Attachment B-2** will be found in the contents of the TARGET PHONE, as described in **Attachment A-2**. The warrant applied for would authorize the copying of electronically stored information under Rule 41(e)(2)(B).

16. Based on your Affiant's training and experience, your Affiant knows that cellular phones are one of the primary modes of communication on the Navajo Nation Indian Reservation. Cellular phones are used to call and text others, as well as to access the Internet. Thus, they can be used to determine or help determine a person's movement prior to a crime and possibly assist in determining the time of an incident and/or time of death.

17. Based on my knowledge, training, and experience, your Affiant knows that cellular telephones contain electronically stored data, including, but not limited to, records related to communications made to or from the cellular telephone, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic "address books;" photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system ("GPS") information.

18. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a cellular telephone, deleted, or viewed via the Internet. Electronic files downloaded to a cellular telephone can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the cellular telephone until it is overwritten by new data.

19. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the cellular telephone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a cellular telephone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

20. As further described in **Attachment B-2**, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cellular telephone was used, the purpose of the use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be found in the contents of the TARGET PHONE because:

a. Data in a cellular telephone can provide evidence of a file that was once in the contents of the cellular telephone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. As explained herein, information stored within a cellular telephone may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove

each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the cellular telephone. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the cellular telephone was remotely accessed, thus inculpating or exculpating the owner. Further, activity on a cellular telephone can indicate how and when the cellular telephone was accessed or used. For example, as described herein, cellular telephones can contain information that log: session times and durations, activity associated with user accounts, electronic storage media that connected with the cellular telephone, and the IP addresses through which the cellular telephone accessed networks and the internet. Such information allows investigators to understand the chronological context of cellular telephone access, use, and events relating to the crime under investigation. Additionally, some information stored within a cellular telephone may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The geographic and timeline information described herein may either inculpate or exculpate the user of the cellular telephone. Last, information stored within a cellular telephone

may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how the cellular telephone was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a cellular telephone that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, cellular telephone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one cellular telephone is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit imaging or otherwise copying the contents of the TARGET PHONE, including the use of computer-assisted scans.

CONCLUSION

22. This affidavit is sworn telephonically before a United States Magistrate Judge legally authorized to administer an oath for this purpose. Based on the foregoing, I request that the Court issue the proposed search warrant because there is probable cause to support that violations of federal law have occurred as described above.

23. Based on the information in this affidavit, your Affiant respectfully submits there is probable cause to believe that evidence described in **Attachments B-1** and **B-2** supporting an investigation related to violations of 18 U.S.C. §§ 1111 and 1153 will be discovered in the residence and TARGET PHONE described in **Attachments A-1** and **A-2**.

Pursuant to 28 U.S.C. § 1746(2), I declare that the foregoing is true and correct to the best of my knowledge and belief.

Jenifer Mulhollen
Special Agent, FBI

6/19/22
Date

Sworn by Telephone

Date/Time: _____

Camille D. Bibles

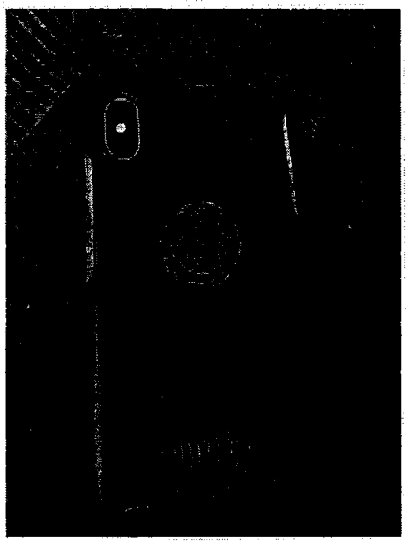
Digitally signed by Camille D. Bibles
Date: 2022.06.19 21:20:56 -07'00'

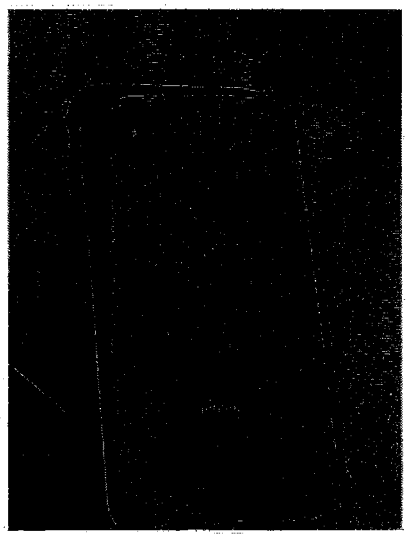
Hon. Camille D. Bibles
United States Magistrate Judge

ATTACHMENT A-2 – PROPERTY TO BE SEARCHED

The property to be searched is a Rose colored iPhone with a purple/pink Otterbox protective case. The TARGET PHONE is currently in the possession of TFO Simonson on scene at milepost 1 on Monument Valley Road in Monument Valley, Arizona.

This warrant authorizes the search of the TARGET TELEPHONE for the purpose of identifying the electronically stored information described in **Attachment B-2**.





ATTACHMENT B-2 – PROPERTY TO BE SEIZED

1. Any records and information found within the digital contents of the TARGET PHONE that relate to violations of 18 U.S.C. §§ 1111 and 1153, including:

a. Content of all text message communications, including deleted messages;

b. Local and long-distance telephone connection records;

c. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

d. All records and other information relating to wire and electronic communications sent or received by the TARGET PHONE, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), SMS detail, email addresses, and IP addresses);

ii. information regarding the cell towers and sectors through which the communications were sent and received.

e. evidence of who used or controlled the TARGET PHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;

f. evidence indicating how and when the cellular telephone was accessed or used to determine the chronological context of the cellular telephone access, use, and events relating to crime under investigation and to the cellular telephone user;

g. evidence indicating the cellular telephone user's state of mind as it relates to the crimes under investigation;

h. evidence of the attachment to the cellular telephone of another storage device or similar container for electronic evidence;

i. passwords, encryption keys, and other access devices that may be necessary to access the cellular telephone;

j. contextual information/data necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the cellular telephone.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.